AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1.   (canceled)

2.   (currently amended)   A method according to claim ~~1~~23, wherein said ~~identifier~~ address token is transmitted in a cookie to said client application.

3.   (currently amended)   A method according to claim ~~1~~23, wherein said ~~identifier~~ address token is received from said client application with said authentication data.

4.   (currently amended)   A method according to claim 3, wherein a new ~~identifier~~ address token is issued to said client application if said authentication data is invalid.

5.   (currently amended)   A method according to claim 4, wherein said ~~identifier~~ address token comprises data indicating the number of times an invalid authenticator has been received from said client application.

6.   (currently amended)   A method according to claim 5, wherein said method comprises ~~issuing~~ transmitting no further ~~identifier~~ address token to said client application if an ~~identifier~~ address token received from said client application indicates that a predetermined number of invalid authenticators have been received from said client application.

7.   (currently amended)   A method according to claim ~~1~~23, comprising timing out said ~~identifier as an identifier~~ address token of an application of a currently authenticated user if no document request is received from said client application for a predetermined period.

8.   (currently amended)   A method according to claim ~~1~~23, comprising authenticating said user for access to a plurality of Web servers located in the same Internet domain; and

enabling each of said Web servers to validate document requests from the client application, which requests include said ~~identifier~~ address token, by checking said status data on receipt of a document request.

9.-22. (canceled)

23.   (new) A method of operating an authenticating server system for

authenticating a user of a client application provided on a client terminal having no unique

IP address via a data communications network, the server system being arranged to control

access to a document stored on a resource server connected to said data communications

network, said method comprising performing the following steps in said server system:

receiving at the resource server a request for said document generated by said client

application;

evaluating at the resource server client-side persistent information accompanying

said request including checking if the client-side persistent information contains an address

token previously issued by the resource server which uniquely identifies the user, and

performing the following steps at the resource server:

i)   if no address token which uniquely identifies the user is contained in the

client-side persistent information accompanying said request:

generating an address token which uniquely identifies the user;

transmitting the generated address token to the client application in a client-

side persistent information packet so that an address token which uniquely identifies

the user is generated and transmitted without prior receipt at the resource server of a

previously issued address token which uniquely identifies the user; and

storing said address token for the user; or

ii)   if an address token which uniquely identifies the user is contained in the client-side persistent information accompanying said request and the address token is an unvalidated address token:

validating the address token using other authentication data received from the client terminal in said client-side persistent information and by reference to user authentication data already stored on said resource server;

storing the validated address token for an authenticated user and an access status of the authenticated user associated with the validated address token; or

iii)   if an address token which uniquely identifies the user is contained in the client-side persistent information accompanying said request and the address token is a validated address token, using said validated address token to enable said resource server to validate said request for said document by checking if said stored access status for said user includes access to said document.

24.   (new) A method as claimed in claim 23, wherein step (ii) further comprises:

transmitting said requested document to said client terminal along with a client-side persistent information packet containing the validated address token to the client terminal.